

Research on the hierarchical protection path of citizens' personal information in the data age by criminal law

Chen Jiankai

Department of Law, Hangzhou Normal University, China
1791691715@qq.com

Received: 31 Aug 2025; Received in revised form: 30 Sep 2025; Accepted: 03 Oct 2025; Available online: 07 Oct 2025

©2025 The Author(s). Published by Infogain Publication. This is an open-access article under the CC BY license

(<https://creativecommons.org/licenses/by/4.0/>).

Abstract—With the rapid development of modern science and technology and the acceleration of digital transformation in society, the era of big data has brought convenience as well as new crimes, and information crimes have become the focus. With the convenience of digitalization, the collection, processing and use of personal information are extensive and in-depth, and information interaction and exposure increase, and criminals illegally use it to infringe on personal and national interests. In the data age, the category of citizens' personal information is huge and the connotation is expanding, and the criminal behavior is diversified, which is difficult for the traditional criminal law protection model to cope with. We should further classify citizens' personal information, coordinate the relationship between criminal law and pre-law, and try to bring new criminal acts into criminal law regulation in order to build a perfect protection system.



Keywords— big data, citizens' personal information, criminal law protection, hierarchical protection

In today's world, a new round of scientific and technological revolution and industrial transformation is in the ascendant, a new generation of digital technology has been vigorously developed and deeply applied, and human society has accelerated into the digital age. The advent of the digital age has brought great convenience to human social life. With digital technology, we can realize fast payment of transactions, fast boarding of vehicles, integrated control of multiple devices, intelligent statistics and distribution of data, etc. However, the foundation of digital convenience is also the collection, calculation and analysis of a large amount of information. The advent of the era of big data has also increased the interaction speed

and exposure frequency of citizens' personal information. Applications installed on mobile phones read and monitor different personal information in the background, and institutions such as schools store a large amount of citizens' information for convenient management. Citizens have gradually become "transparent people" in the digital age. At the same time, the number of crimes committed by criminals using citizens' personal information has increased sharply, and the criminal means are diversified. The traditional criminal law has exposed some limitations in protecting personal information and cracking down on new information crimes, and the criminal law protection of personal information needs to be further explored.

I. CITIZENS' PERSONAL INFORMATION IN THE ERA OF BIG DATA

1.1 The era of big data

Today's society is developing at a high speed and technology is developed. The era of big data is no longer a new and unfamiliar term, but it is already our era. In the era of big data, the efficient integration and in-depth application of data information and intelligent technology not only significantly enhances the accuracy and efficiency of personal and commercial applications, but also strongly promotes the comprehensive optimization and sustainable development of emerging cities in terms of planning and layout, construction and implementation, management and operation.^①In the major commercial and economic fields, with the help of algorithms, cloud technology, Internet of Things, artificial intelligence, etc., information data can be accurately analyzed and processed, and accurately delivered to the target group. Personal information no longer only carries personal privacy and personality, but also reflects great economic value. In the era of big data, personal information no longer stays in traditional information such as names, home addresses and contact numbers that can be easily obtained, but also covers more secret and sensitive information such as whereabouts and property status. They are stored in different systems in the form of electronic data in different ways, just like storing natural persons directly in a library. In the era of big data, citizens' personal information has a clear directivity, and its connotation and extension have been extended. This also shows that while information and data interact and circulate at high speed in the data age, it also leaves hidden dangers of "targeted illegal use" at different levels.^② With the increase of illegal use of information by criminals, more unknown risks lurk in the era of big data and the information society, and the protection of citizens' personal information has become an important topic of contemporary rule of law protection and data order maintenance.

^① Gao Fuping: "On the Purpose of Personal Information Protection —— Focusing on the Differentiation of Interests in Personal Information Protection Law", *Law and Business Research*, No.1, 2019.

^② Yang Nan: *Functional Errors and Amendments in Criminal Law Regulation of Personal Digital Footprints*, *Journal of Anhui University (Philosophy and Social Sciences Edition)*, No.4, 2019.

1.2 Personal information of citizens

Personal information refers to a collection of symbols related to individuals, which reflects the facts or state of individuals, has the structural and hierarchical characteristics of information, and can be felt and recognized by people.^③That is, a recognizable symbol system that is associated with people and reflects individual characteristics.^④In the era of big data, in order to better realize the special protection of criminal law, it is first necessary to clarify the legal interests of citizens' personal information. There have been different views in theory and practice.

Some people think that citizens' personal information mainly belongs to the legal interests of property rights, similar to those stipulated in the civil law, and citizens have the corresponding rights to possess, use, benefit and dispose of their personal information. We should admit that with the development of emerging technology and information society, citizens' personal information presents unprecedented economic value. Information holders can legally process and analyze the information to identify it, and then integrate it and sell it to the corresponding enterprises. Enterprises can use the processed information to find their customer groups and provide them with accurate services, so as to obtain huge commercial profits and form a win-win cycle model. However, the limitation of this view is that it does not realize the personality right attribute contained in citizens' personal information, and only treating information as a property attribute will damage personal personality and be suspected of materialization. Although there are individual differences among citizens, the value of their personal information will also show different differences, but it should be equally protected under the law. Some scholars believe that the legal interest attribute of citizens' personal information protected by criminal law belongs to privacy.^⑤ The theory holds that citizens' personal

^③ Gao Fuping, Wang Wenxiang: *The Boundary of Criminalization of Selling or Providing Personal Information of Citizens*, *Politics and Law*, No.2, 2017.

^④ Wang Liming: *On the Position of Personal Information Right in Personality Right Law*, *Journal of Suzhou University (Social Science Edition)*, No.6, 2012.

^⑤ Cai Jun, *Rational Analysis on Legislation of Crime of Infringement on Personal Information —— Reflection and Prospect on Legislation of this Crime*, *Modern Law*, No.4, 2010.

information belongs to the category of privacy and can effectively resist illegal interference, intrusion and utilization by others. However, in the era of big data, citizens' personal information is relatively dynamic, which will change its attributes with different scenarios, and the scope of privacy is difficult to define. Too much emphasis on the legal interest attribute of privacy will also lead to some citizens' personal information not being protected as it should be.

There is also a view that nowadays, citizens' personal information has both personality and property attributes, and the right to personal information should be protected as an independent right. The right of personal information is the basis of citizens' personal information protection, and the protection of personal information itself is the protection of citizens. From the generation principle of personal information, personal information represents the externalization of citizens' personal attributes, that is, the extension of citizens' individuals. Although this right has not been clearly listed in China's Civil Code, it can be inferred that this right belongs to a separate right through system analysis.^① On the basis of determining the right of personal information, it is proposed that the legal interest of criminal law in protecting citizens' personal information is the right of information self-determination under the right of personal information. Citizen's authorization of information is the fundamental source of information's right to be used in the subsequent circulation process, and the existence of information's right to self-determination is the absolute premise for information to be used reasonably and to ensure the reasonable distribution of interests of all parties.^② Citizens have the right to decide what to do with their information. The right to information self-determination is the basic legal interest protected by the crime of infringing citizens' personal information. The scope of citizens' authorization for personal information determines the extent to which illegal use of personal information should be regulated, and at the same time provides a legitimate basis for social information

governance and a pre-existing basis for maintaining the circulation order of personal information in society.^③ The author believes that the theory based on the right to self-determination of information in the era of big data can provide a more accurate and comprehensive protection path in the face of different types of information, and provide corresponding legal protection for citizens' personal information while adhering to the principle of modesty of criminal law. It also reflects that we should build a hierarchical protection system for citizens' personal information in criminal law, that is, protect personal information at different levels, not just focusing on unilateral rights, so as to better play the role of regulation and protection of criminal law.

II. THE DILEMMA OF CRIMINAL LAW PROTECTION OF CITIZENS' PERSONAL INFORMATION IN THE DATA AGE

2.1 the convergence of criminal law and pre-existing law is not smooth

In the current legal framework for the protection of citizens' personal information, the protection of criminal law should focus on the coordination and connection with the pre-law. With regard to the connection between pre-law and criminal law, the provisions of pre-law cannot be directly used as the basis for judging whether an act constitutes a crime in criminal law. Specifically, the prohibitive provisions in the pre-law, as a supplement to the openness of criminal law norms, have become one of the key bases for evaluating whether an act constitutes a crime. At the same time, the upper limit of liability set by the pre-law and the lower limit of liability set by the criminal law should be connected in a reasonable and organic way, that is, through the theory of legal interests: only when the relevant illegal acts identified by the current law infringe on the protection interests under the criminal law norms can they be identified as crimes. This process ensures the consistency and rationality within the legal system and helps to better safeguard the personal information security of citizens. Therefore, the normative

^① Liu Yanhong: Protection Benefits of Crimes against Citizens' Personal Information in the Context of Civil Code Compilation: Right to Information Self-determination, *Journal of Zhejiang Gongshang University*, No.6, 2019.

^② Ma Yongqiang: Confirmation of the Legal Interest Attribute of the Crime of Infringing Citizens' Personal Information, *Global Law Review*, No.2, 2021.

^③ Zhao Tong: Circle-type Criminal Law Protection of Personal Information under the Structure of Double Legal Interests, *Journal of Southeast University (Philosophy and Social Sciences Edition)*, No.4, 2024.

relationship between the prohibitive provisions of the preceding law and the norms of criminal law can be summarized as follows: if the act that violates the prohibitive provisions of the preceding law does not infringe on the protection interests of the criminal law norms, the actor will only bear civil or administrative responsibilities; If the behavior that violates the prohibitive provisions of the preceding law infringes on the legal interests protected by the criminal law norms at the same time, the behavior can be included in the scope of criminal law regulation, and the actor can bear criminal responsibility.

China's Civil Code clearly distinguishes personal information from private information in the compilation of personality rights. Later, the Personal Information Protection Law clearly divided citizens' personal information into general personal information and sensitive personal information, and specially protected sensitive personal information. However, the Criminal Law does not further distinguish personal information, and the Interpretation of the Two Highs only defines "citizen's personal information" as "all kinds of information recorded by electronic or other means that can identify a specific natural person or reflect the activities of a specific natural person alone or in combination with other information, including name, ID number, communication contact information, address, account password, property status, whereabouts and so on. In order to maintain the unity of legal order, better protect personal information and establish a perfect preventive mechanism, it is an urgent practical problem how to protect personal information in criminal law.

2.2 The scope of criminal law protection of personal information is limited.

Although the criminal legislation on the protection of personal information was made earlier in China, the crime of infringing citizens' personal information stipulated in Article 253 of the Criminal Law of China: "Whoever sells or provides citizens' personal information to others in violation of relevant state regulations, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years, and shall also be fined ..." However, this article does not limit the scope of personal information accordingly, that is,

all citizens' personal information shall be protected by criminal law from the perspective of literal interpretation. The subsequent Interpretation of Two Highs further explains this. Article 5 of this Interpretation divides citizens' personal information into three levels: the first level is track information, communication content, credit information and property information; The second level is other accommodation information, communication records, health and physiological information and transaction information that may affect personal and property safety; The third level is the personal information of other citizens. However, the author believes that in the era of big data, not all personal information should be generally included in the protection of criminal law. The purpose of criminal law is to protect interests, but not all legal interests are protected by criminal law, and only when they are violated by "out of the scope of social life order and worthy of punishment" are they protected by criminal law.^①

Under the background of information society, the utility of personal information becomes more and more prominent. In the information age, we not only deeply realize the value attribute of information itself, but also emphasize the great benefits and positive influence that the rational use of information can bring to society. However, emphasizing information utilization does not mean that we only need to focus on the protection of sensitive information and ignore general information. Whether it is general information or sensitive information, it is an important part of personal privacy and rights, and it needs to be equally valued and properly protected. It is precisely because of the social openness of general information that rational utilization can quickly enhance social benefits and promote economic and social development that the era of big data can be established. At the same time, from the perspective of protection cost, the amount of general information is numerous and not all of them have protection value. If excessive protection is carried out, it will not only be difficult to achieve the protection effect, but also bring huge loss of judicial resources. If citizens' personal information is indiscriminately protected by criminal law, it will also hurt the prestige of criminal law.

^① Wei Hantao: Deviation and Rectification of Criminal Law Protection of Citizens' Personal Information, Law Review, No.4, 2024.

On the contrary, weak protection of general information is beneficial to the development of the information subject itself. For example, the information subject can obtain the content it needs in time, and the utilization and value are greater than the protective demand.

Sensitive information needs criminal law protection. Sensitive personal information is closely related to major rights and interests. Once sensitive information is leaked or infringed, it often directly touches the core of citizens' personal dignity. The main goal of protecting citizens' personal information in criminal law is to protect their personal rights and property rights. Different types of personal information are closely related to citizens' personal and property rights, so violations of different types of personal information will not show different social harmfulness.^① Because sensitive personal information is closely related to personal dignity, personal rights and property rights, sensitive personal information should appear in the field of criminal law protection. Non-sensitive personal information, such as the personal height and weight of citizens, has relatively limited use value directly presented or indirectly identified, and it is difficult to become the target of infringement by criminals. Even if this information is infringed, the potential harm is relatively small, and it can usually be effectively handled and regulated at the civil and administrative levels. The protection of this kind of information is important, but because of its low risk, at the legal level, it depends more on civil and administrative regulations for management and prevention, and criminal law can invest more resources to protect other information with higher risks.

2.3 the limitations of the traditional mode of collateral protection

For the protection of personal information, the criminal law of our country stipulated the crime of infringing citizens' personal information earlier. In view of the low popularity of the internet at that time, citizens were more exclusive about their personal information, and the degree of distinction between personal information and other types of information was not high. At this time, the security of personal information was indirectly protected

through macro-order protection. However, in the era of big data, the right to personal information has been separated from the right to privacy and has become a new personality right. It cannot be ignored that the formation and development of personal information right is closely related to the theoretical framework of privacy right. In the traditional legal system, personal information has long been included in the category of privacy and regarded as an important dimension of privacy. With the advent of the information age, the connotation and extension of personal information are constantly expanding, and its position in legal protection is gradually prominent. The emergence of personal information right is the concrete application and logical extension of privacy right under the background of information age, and there is a close relationship and interaction between them.^② After the promulgation of the Personal Information Protection Law, China's current laws have clearly defined the right to privacy and the right to personal information as two coexisting personality rights.^③ From the nature of rights, the right to privacy is an absolute right, which is manifested in the absolute control of personal privacy and the right to exclude illegal interference from others, while the right to personal information is more focused on a positive right, such as the right to know, the right to delete, the right to block, etc., which is the balance and control of individuals in the use and protection of their information.^④ At present, the connotation and extension of personal information have changed. With the scene changing, it presents different properties and has independent value. In the past, the incidental protection mode can no longer regard privacy and exclusiveness as the proper characteristics of personal information, and personal information forms an independent characteristic of non-exclusive and public sharing, which is different from privacy. Personal information cannot be protected simply by the regulation means of privacy or exclusiveness as the core.^⑤ Secondly,

^② Shi Jiayou: Rethinking the Relationship between Privacy and Personal Information, *Journal of Shanghai University of Political Science and Law (On the Rule of Law)*, No.5, 2021.

^③ Cheng Xiao: On the Relationship between Personal Information Rights and Privacy, *Contemporary Law*, No.4, 2022.

^④ Baiyun: The Legal Nature of Personal Information Rights, *Credit Information* No.2, 2020.

^⑤ Li Jie: How to Protect Privacy in Criminal Law — Comment on the Personal Information Protection Clause of Criminal Law Amendment (IX), *Journal of Jinan (Philosophy*

^① Liu Xianquan: Research on Special Protection of Sensitive Personal Information in Criminal Law, *Law Review*, No.3, 2022.

in the data age, personal information presents the types of sensitive information due to information exchange and other reasons. Sensitive information does not necessarily belong to private information, and there is some overlap between them. However, the extension of sensitive information is larger and more flexible, and it is difficult for the traditional mode of incidental protection of criminal law to cover the protection of different types of information in the data age. Furthermore, the criminal means and subjects of information cases are diversified, and it is difficult to incorporate some new types of behavior into the current norms of criminal law, such as the "abuse" of massive information, which may lead to a series of chain risk consequences. Faced with such a situation, criminal law needs to protect personal information at different levels, and at the same time, re-examine the control strategies of various behaviors, adjust the regulation path of criminal acts accordingly, and explore new information protection models.

III. THE CONSTRUCTION OF HIERARCHICAL PROTECTION PATH OF DATA INFORMATION IN CRIMINAL LAW

3.1 to strengthen the coordination and convergence with the pre-method

Regarding the protection of citizens' personal information, China has successively promulgated the Civil Code and the Personal Information Protection Law in the civil and administrative fields, and there is already a relatively perfect pre-existing legal system. Although the criminal law and other departmental laws have different legal relations and different emphases, in order to maintain the unity of legal order and consolidate the protection foundation of citizens' personal information, the criminal law needs to realize the coordinated relationship with the pre-law on the premise of adhering to modesty. The Civil Code adopts the definition of personal information and private information, and the Personal Information Protection Law, as an important pre-law, adopts the dual classification protection mode of sensitive information and general information. However, neither the Criminal Law nor the Interpretation of the Two Highs have made

significant provisions on the classification of personal information.

The author believes that the Criminal Law should also adopt the dichotomy between sensitive information and personal information to build a special protection system, which can adopt the following two paths: one is to add the relevant provisions of the crime of infringing citizens' personal sensitive information, so as to reflect the special protection of sensitive information in a more targeted way. The second is to add "citizens' personal information includes citizens' general personal information and citizens' sensitive personal information" to the crime of infringing citizens' personal information in Article 253 of the Criminal Law, so as to realize the corresponding connection with the Personal Information Protection Law, define the scope of citizens' personal information in a consistent way, and at the same time highlight the criminal law's attention to sensitive information. However, in contrast, the first path is simple and rude, but it needs more consideration. For example, if new types of information are derived in the process of continuous development in the era of big data, adding and modifying criminal law charges at will will damage the prestige of criminal law, while the second path can also achieve better results by fine-tuning the existing charges.

Under the coordination of macro-pre-law, it is also a feasible starting point to improve industry rules and self-discipline, which can help the pre-law and criminal law to protect citizens' personal information more coherently. The industry self-discipline standard is a set of professional and perfect rules formed by the industry itself, which is self-restraint and regulation of the relevant industry subjects within the scope of private law. It has a certain binding effect on the practitioners in the relevant industries. In the case of immature law, it takes into account the modesty and lag of criminal law and sets a strong protective barrier for preventing citizens' personal information crimes. In the era of big data, citizens' personal information is often collected and stored in various business units, and depends on the analysis and processing of these subjects. Although the industry self-discipline rules are not mandatory, they can achieve good protection results at a good economic cost. At the same time, it is more helpful to include the obligations and

judgment rules of employees in professional industry self-discipline standards in the scope of measuring the harmfulness of behavior. On the one hand, related industries can formulate more targeted and detailed guidelines for the protection and utilization of personal information according to the principles of the current pre-law, combined with their actual business conditions and specific work needs. These guidelines can not only provide more convenient, comprehensive and high-level protection for information subjects, but also ensure that enterprises can better carry out business activities on the basis of legal compliance. On the other hand, the autonomous supervision mechanism implemented through the unique flexibility, synergy and technological innovation of the Internet industry can make up for the possible supervision gaps in legal norms to some extent. Through the continuous improvement of industry rules and the support of improving the level of industry self-discipline, criminal law will be able to achieve an effective connection with the pre-law more smoothly and jointly build a more sound and efficient personal information protection system.

3.2 Emphasis on classified protection of information

As mentioned above, in the era of big data, there are different types of information, and different types of information need different degrees of protection. On the basis of pre-law, criminal law should also establish a hierarchical protection system for information. In the Interpretation of the Two Highs, the "serious circumstances" of the crime of infringing citizens' personal information have made different provisions on the classification of different kinds of information, such as the requirement of information quantity, which also shows that there is a momentum of information classification protection in criminal law. Sensitive information is highly related to citizens' personal dignity and personal property safety, so it should be emphasized to take sensitive information as the starting point for hierarchical protection. Some scholars argue that the protection of sensitive personal information should be cancelled because its importance will change with different scenes.^①However,

the author thinks that the primary and secondary logic of this view is vague. No matter how the scene changes, it is necessary to judge the real risk of sensitive information, rather than deciding whether to protect it by the scene. On the contrary, this is the original intention of establishing hierarchical protection.

Just because different types of sensitive personal information are subjected to illegal acts does not mean that different sensitive personal information is used to infringe citizens' personal rights and property rights at the same risk. According to the governance jurisprudence of risk crime, the higher the risk of infringing on legal interests, the lower the threshold of conviction; or vice versa, Dallas to the auditorium^②For personal information with high protection requirements, a heavier penalty and a lower conviction threshold are stipulated. On the contrary, for personal information with low protection requirements, a lighter penalty and a lower conviction threshold are adapted. Such graded protection requirements not only emphasize the special protection of certain information, but also reflect the adaptation of crime and punishment. Furthermore, the fundamental reason why citizens' personal information has attracted much attention is that the risk of personal information being abused increases in the data age, and classified protection of information is necessary and the general trend. The author thinks that we can improve the existing provisions in the Interpretation of the Two Highs to better construct classified protection. One is to clarify the specific criteria for judging two levels of sensitive personal information, so as to define the protection scope of different levels of personal information more accurately. For low-sensitive personal information, it can be summarized as "personal information that, once leaked or illegally used, is relatively easy to cause personal dignity of natural persons to be violated, or poses certain harm to their personal and property safety". Although the sensitivity of this kind of information is relatively low, once it is leaked or abused, it may still cause some troubles and losses to individuals. For highly sensitive personal information, the judgment standard is stricter, which can be summarized as "those personal information that, once leaked or illegally used, can easily lead to serious

^① Liu Xianquan: Research on Special Protection of Sensitive Personal Information in Criminal Law, Law Review, No.3, 2022.

^② Wei Hantao: Reflection and Reconstruction of the Relationship between Crime and Punishment, Politics and Law, No.4, 2019.

violations of the personal dignity of natural persons or pose a major threat to their personal and property safety". This kind of information usually involves the core privacy and rights of individuals, and once it is leaked or abused, the consequences will be unimaginable. In this way, the information classification is clear, which provides a basis for further refinement. Secondly, the Interpretation of the Two Highs stipulates the provisions of "serious circumstances" and "particularly serious circumstances", but it may be inappropriate to take 10 times the standard of the number of convictions as the standard for upgrading the statutory punishment, because in information crime cases in the information age, the number of information is often thousands or tens of thousands or even worse, and the standard of 10 times is difficult to distinguish between ordinary crimes and serious crimes, which will also make the perpetrator suffer heavier punishment without causing actual damage, which is contrary to the punishment of guilt.

3.3 the "abuse" behavior into regulation

In the era of big data, with the continuous updating and changes of criminal means, the traditional mode of incidental protection of criminal law has been difficult to meet the needs of the times. In the theory of hierarchical protection, information protection means is also an important angle to be considered. In the case of information crimes in the data age, actors such as enterprises, telemarketers and server managers often control a huge amount of information, which easily leads to "abuse" behavior patterns. However, in the crime of infringing citizens' personal information, the Criminal Law only stipulates two behaviors: selling and providing information, and the Interpretation of the Two Highs does not include the common behaviors of information abuse in the data age. "Abuse" refers to the indiscriminate or excessive use, which often follows the act of selling and providing, such as wantonly spreading citizens' personal information for telecom fraud. Under the norms of pre-law, this behavior type can not be well regulated. From the perspective of civil law, when personal information is abused, civil law cannot accurately determine the standard and scope of compensation, and it is difficult to effectively deal with the widespread fears and risks caused by it,

which makes victims face many difficulties in king relief.^①. On the other hand, although administrative law norms can curb information "abuse" to a certain extent, their deterrent power is far less than that of criminal law. If the criminal law regulates "abuse" means and sets strict punishment measures, it can more effectively stop the behavior of potential criminals. Once potential offenders realize that they will face severe criminal responsibility, they usually reconsider and finally decide to give up such behavior. This powerful deterrent effect is difficult to achieve by other departmental laws.

The author thinks that criminal law can further refine the behavior of this crime and classify "abuse" into criminal law regulation. First of all, according to the Interpretation of the Two Highs, "abuse" behavior cannot be included in serious circumstances. The category of "serious circumstances" and "abuse" cannot be included in it by using literal interpretation methods or similar interpretation rules. Secondly, abuse, as a common behavior in the data age, is quite harmful to the "acquisition" and "sale" of citizens' personal information, and should be restrained and regulated. Furthermore, as the second-order behavior of "acquisition" and "sale", the subject of "abuse" may be separated, and the citizen information at this stage may be highly sensitive, which may easily lead to some panic, such as maliciously changing the face of relatives and friends through intelligent technology to commit fraud, which will not only cause serious harm to individuals, but also have a negative impact on the whole society. Incorporating "abuse" into the criminal law is conducive to cracking down on the industrial chain of information crimes, further improving the protection mechanism of information classification protection, and protecting sensitive information and safeguarding social order and citizens' rights and interests.

IV. CONCLUSION

Citizens' personal information is closely related to their personal freedom and dignity. In the era of big data, the amount of information is larger than in the past,

^① Yang Chunran: On the Criteria for Dividing Criminal Law Boundaries, China Journal of Criminal Law, No.8, 2012.

information processing and interaction are more frequent, and the value of citizens' personal information is also increasingly prominent. With the development of science and technology, the types of information crimes are frequent, and the criminal means are diversified. The security of personal information has become an important issue. From the addition of the crime of infringing citizens' personal information in the amendment to the promulgation of "Two High Interpretations", China's criminal law has been committed to the protection of personal information, but there are still some problems to be solved urgently. For example, how to balance the relationship between coordination and prepositional law in criminal law when the existing prepositional law is relatively perfect; In the information society, personal information presents different types, and the criminal law has not yet formed a perfect hierarchical protection system; How to adjust the protection path and bring "abuse" into the scope of regulation in the case that the traditional criminal law incidental protection model is difficult to cover modern information protection. In the data age, it is difficult for us to predict the real trend in the future. We need to start from more breakthrough points and improve the protection system of citizens' personal information in criminal law.

REFERENCES

- [1] Gao Fuping: "On the Purpose of Personal Information Protection —— Focusing on the Differentiation of Interests in Personal Information Protection Law", *Law and Business Research*, No.1, 2019.
- [2] Yang Nan: Functional Errors and Amendments in Criminal Law Regulation of Personal Digital Footprints, *Journal of Anhui University (Philosophy and Social Sciences Edition)*, No.4, 2019.
- [3] Gao Fuping, Wang Wenxiang: The Boundary of Criminalization of Selling or Providing Personal Information of Citizens, *Politics and Law*, No.2, 2017.
- [4] Wang Liming: On the Position of Personal Information Right in Personality Right Law, *Journal of Suzhou University (Social Science Edition)*, No.6, 2012.
- [5] Cai Jun, Rational Analysis on Legislation of Crime of Infringement on Personal Information —— Reflection and Prospect on Legislation of this Crime, *Modern Law*, No.4, 2010.
- [6] Liu Yanhong: Protection Benefits of Crimes against Citizens' Personal Information in the Context of Civil Code Compilation: Right to Information Self-determination, *Journal of Zhejiang Gongshang University*, No.6, 2019.
- [7] Ma Yongqiang: Confirmation of the Legal Interest Attribute of the Crime of Infringing Citizens' Personal Information, *Global Law Review*, No.2, 2021.
- [8] Zhao Tong: Circle-type Criminal Law Protection of Personal Information under the Structure of Double Legal Interests, *Journal of Southeast University (Philosophy and Social Sciences Edition)*, No.4, 2024.
- [9] Wei Hantao: Deviation and Rectification of Criminal Law Protection of Citizens' Personal Information, *Law Review*, No.4, 2024.
- [10] Liu Xianquan: Research on Special Protection of Sensitive Personal Information in Criminal Law, *Law Review*, No.3, 2022.
- [11] Shi Jiayou: Rethinking the Relationship between Privacy and Personal Information, *Journal of Shanghai University of Political Science and Law (On the Rule of Law)*, No.5, 2021.
- [12] Cheng Xiao: On the Relationship between Personal Information Rights and Privacy, *Contemporary Law*, No.4, 2022.
- [13] Baiyun: The Legal Nature of Personal Information Rights, *Credit Information* No.2, 2020.
- [14] Li Jie: How to Protect Privacy in Criminal Law —— Comment on the Personal Information Protection Clause of Criminal Law Amendment (IX), *Journal of Jinan (Philosophy and Social Sciences Edition)*, No.12, 2016.
- [15] Liu Xianquan: Research on Special Protection of Sensitive Personal Information in Criminal Law, *Law Review*, No.3, 2022.
- [16] Wei Hantao: Reflection and Reconstruction of the Relationship between Crime and Punishment, *Politics and Law*, No.4, 2019.
- [17] Yang Chunran: On the Criteria for Dividing Criminal Law Boundaries, *China Journal of Criminal Law*, No.8, 2012.